Section 5. Standards and Systems

The trends in facilities design have resulted in a greater emphasis on the need for standards. Through standards, design consultants and school planners can be sure the infrastructure and systems will successfully support the anticipated increased reliance on technology. By adopting standards in the foundation of the facility design, the fast-paced and constantly changing nature of the new technology systems built on this foundation can be more efficiently planned, constructed and managed.

Learning environments are becoming more modular, transformable and mobile as the boundaries between teachers and learners become more permeable. It is important to adopt industry standards and guidelines in order to best serve these environments and emerging technology systems. It is the purpose of this section to address these standards and to address the physical aspects of the design and planning for technology infrastructure.

I. Standards

Integration of technology is a key element of school building design. Administrators and design professionals need to make a concerted effort to intelligently plan and locate building systems as they become increasingly critical to the operation and day-to-day functioning of the facilities. This becomes evident as components such as voice systems (e.g. VoIP systems), Audio-Visual and security systems converge on to the network infrastructure.

A. Code vs. Standard - Definition

A code is a set of minimum regulations and requirements that an architect is legally bound to follow. A standard is an agreed set of principles and protocols that groups voluntarily follow.

B. Compliance Codes Examples

ICC/BOCA - The International Code Council (ICC) is a compilation of several code authorities including the Building Officials and Code Administrators who published the BOCA National Building Code series. New Jersey was under BOCA but now has adopted the International Code Council's NJ International Building Code along with associated codes.

N.J.A.C. – The New Jersey Administrative Code is relevant as it relates to technology proposes and adequately implementing the Core Curriculum Content Standards in Technological Literacy. Technological literacy includes both computer and information literacy and technology education. Integration of technological literacy should occur at all grade levels.

NEC (National Electrical Code) – Article 645. The most widely adopted element of a building code in the United States and the world, the National Electrical Code is the benchmark for safe and efficient cabling installations.

C. Additional Standards and References

The standards that are used for technology infrastructure design and construction have arisen out of necessity and demand from the design, installation and construction community.

ANSI - The American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system for more than 90 years. Founded in 1918 by five engineering societies and three government agencies, the Institute remains a private, nonprofit membership organization supported by a diverse constituency of private and public sector organizations. ANSI's common principles of understanding and guidelines include development of industry standards, as well as the standards and needs of network applications, users, content and information providers. They also include international standards matters, cross-industry cooperation and the role of government and architectural process and analysis.

ANSI standards are referenced in almost all product and project specifications with items, including, but not limited, to fiber optic connectivity, copper cabling standards and storage area networks.

EIA/TIA – Electronics Industry Assoc./Telecommunications Industry Assoc.

Published in July of 1991, the EIA/TIA 568, 569, 606 and 607 standards serve the following purposes:

- Specifies generic telecommunication cabling system which supports multi-product, multi-vendor environments.
- Provides direction for commercial telecommunication product design.
- Enables planning and installation of cabling with minimum knowledge of the telecommunication products to be installed.
- Establishes performance/technical criteria for various cabling system configurations.

The EIA/TIA Standard specifies:

- Minimum requirements for telecommunications cabling within an office environment.
- Recommended topology and distances.
- Media parameters which determine performance.
- Connectors and pin assignments to ensure interconnection ability.
- The useful life of telecommunications cabling systems as being in excess of ten years.

BICSI – Building Industry Consulting Service International

BICSI is a widely recognized leading professional association supporting the information infrastructure industry with information, education and certifications for individuals and companies.

NJ Department of Community Affairs (DCA) – Best Practices Standards for Schools Under Construction or Being Planned for Construction.

DCA has established security-related requirements that the design consultant **must follow** on new facility projects. The requirements encompass the following areas:

- Site Layout
- Building Layout
- Specific Standards regarding:
  - Exterior Lighting
  - Entrance access
  - HVAC
  - Fire Protection
  - Elevators
  - Emergency Control Center and Communications
  - Video Surveillance

The most current version of the best practice guidelines is available at http://www.state.nj.us/dca/codes/misc/pdf/ed_bp_stndrs_11_10_2008.pdf

Design consultants and IT planners shall verify with the DCA that they are using the most current applicable version of the best practice requirements. The technology disciplines most directly affected by the DCA requirements are Security and Telecommunications. Refer to Section 3 of this document for more detail on how these requirements are to be incorporated into the facility design and project deliverables.

ADA Compliance, Design for Inclusion and Technology (American with Disabilities Act)

In 1998, Congress amended the *Rehabilitation Act* to require agencies to make their electronic and information technology accessible to people with disabilities. "Inaccessible" technology interferes with an individual's ability to obtain and use information quickly and easily. This was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities and to encourage development of technologies that should help achieve these goals.

D. Applying Standards

1. **Adherence to Standards**
   When there are industry or district standards addressing an item, such standards, wherever feasible, should be included in the requirements of the standard item.

2. **Flexibility**
   End users of technology usually have varying needs for digital tools and would like as much flexibility as possible in selecting the optimum product for each need. Whenever possible, the criteria for selecting standards should provide as much flexibility to the user as possible. When such flexibility is insufficient to meet the user's need, the technology standards procedures allow a waiver process for proprietary items allowing purchase of a non-standard item.

3. **Expandability**
   Standards should allow for the capability of expansion in order to meet growth. If the expansion requires the purchase of additional items, these items should fall under standards process control.

4. **Support for Existing Resources**
   Standards must require interoperability and compatibility with the existing infrastructure and any existing items that might interact with the standard item. Where possible, qualification testing should be required to assure interoperability.

5. **Reliability/Availability**
   For hardware items, the standard should include minimum acceptable reliability and availability requirements.

6. **Data Security**
   Standards should include specifications for ensuring network security, whenever applicable. For example, the proliferation of wireless telephones and wireless computers poses security risks that requires their inclusion under standards process control.

7. **Cost of Ownership**
   The standard should include any requirements that can lower the total cost of ownership while meeting the minimum requirements of the users.

8. **Performance**
   Standards should specify parameters for minimum acceptable performance in order to ensure the user requirements.

E. District Educational Technology Plan (Three Year Plan)

The New Jersey Department of Education recommends that each district have an approved educational technology plan. Also, the Federal Communications Commission requires district technology plans for certain funding programs such as E-Rate. To ensure that schools are prepared to effectively use the technology services, districts must certify that their requests are based on approved technology plans and include provisions for integrating telecommunication

services and Internet access into their educational programs. Most schools have already developed such plans and may only need to modify these existing plans to conform to program criteria for technology plans. The plan must establish clear goals and a realistic strategy for using telecommunications, information technology and digital tools to improve educational services. Districts who seek E-Rate funding for telecommunication services should review the following information about technology plan requirements and approval:

- The plan must have a professional development strategy to ensure that staff is trained to use these new technologies to improve education services;
- The plan must include an assessment of the telecommunication services, hardware, software, and other services that will be needed to improve education or library services;
- The plan must provide a sufficient approved budget to acquire and support the non-discounted elements of the plan - the hardware, software, professional development and other services that will be needed to implement the strategy; and
- The plan must include an evaluation process that enables the school to monitor progress toward the specified goals and make mid-course corrections in response to new developments and opportunities as they arise.

F. Specification Format – CSI Division 27 and 28

As the complexity and details for technology systems have grown, so has the importance of adhering to the CSI MasterFormat, the U.S.-Canadian standard for organizing specifications and other data for commercial and institutional buildings. MasterFormat 2004 Edition, released in November 2004 by the Construction Specifications Institute (CSI) and Construction Specifications Canada, has been greatly expanded beyond the previous edition to include significant changes in design, construction and management of facilities.

As a matter of practice, districts and design consultants may adopt and utilize this revised CSI MasterFormat 2004. The revision includes a new series called "Facility Services" that is numbered in the 20's. For example, mechanical and electrical, formerly Divisions 15 and 16, now are in this section, along with an area referred to as "CLA" (**c**ommunications, **l**ife safety, integrated **a**utomation systems).

Below is an outline of Division 27 (Communications) and Division 28 (Electronic Safety and Security) that may be considered and used for project specifications.

DIVISION 27 – COMMUNICATIONS

270500 - COMMON WORK RESULTS FOR COMMUNICATIONS
Materials and methods common to multiple communication systems.

271100 - COMMUNICATIONS EQUIPMENT ROOM FITTINGS
Telecommunications mounting equipment, service pathways, and grounding.

271300 - COMMUNICATIONS BACKBONE CABLING
Pathways, cables, connecting hardware, and cable identification systems.

271500 - COMMUNICATIONS HORIZONTAL CABLING
Pathways, cables, connecting hardware, and identification and administration systems.

272000 – DATA COMMUNICATIONS
Network equipment, hardware, peripheral data equipment, software and programming and integration services

273000 – VOICE COMMUNICATIONS
Switching and routing equipment, telephone sets, facsimiles, modems, messaging, call accounting and call management

274100 – AUDIO-VIDEO SYSTEMS
Integrated audio-video systems for classrooms, theaters, auditoriums, conference rooms, stadiums and arenas

274133 - MASTER ANTENNA TELEVISION SYSTEM MATV
Options for off-air antennas, CATV, or broadcast satellite service.

275113 – PAGING SYSTEMS
Overhead paging, public address and mass notification systems

275313 - CLOCK SYSTEMS
Master and secondary clocks and signal devices; interface with intercom and public address systems

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

280500 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY
Materials and methods common to multiple electronic safety and security systems.

280513 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY
UTP, fiber-optic, coaxial, RS-232, and RS-485 cables, connecting hardware, and identification systems.

281300 - ACCESS CONTROL
Computer controlled, with interface to other facility management systems.

281600 - INTRUSION DETECTION
Detection devices, controls, and alarms.

281643 - PERIMETER SECURITY SYSTEMS
Detection devices, controls, and alarms on the site perimeter.

282300 - VIDEO SURVEILLANCE
Cameras, data transmission wiring, monitors, and control equipment.

283111 - DIGITAL, ADDRESSABLE FIRE-ALARM SYSTEM
Systems with addressable initiating devices and conventional or addressable notification appliances.

283112 - ZONED (DC LOOP) FIRE-ALARM SYSTEM
Small systems for buildings relying on zoned fire alarm concept.

283500 - REFRIGERANT DETECTION AND ALARM
Monitors, alarms, breathing apparatus, and ventilation equipment interlocks.

284619 - PLC ELECTRONIC DETENTION MONITORING AND CONTROL SYSTEMS
Monitoring and control of doors, gates, and related items for detention facilities.

II. Communications Services and Systems

This section examines specific technology services, systems, areas or concepts. Each item will be defined and an example or current industry standard will be included. These design concepts and standards are applicable to new construction and sizable additions and renovations. Smaller-scale projects and retrofits can also use these standards as a guideline to be incorporated accordingly by the district and their design team.

Definitions for certain IT spaces are changing and are used interchangeably. The space where communications cables enter the building and terminate is called the "MDF" (main distribution frame) and the space on each of the floors where the voice and data cables terminate is called the "IDF" (intermediate distribution frame). Small telecom spaces have historically been called "closets". These terms were originated by AT&T in the 1960s. While these terms hardly describe what actually goes on in these spaces, the nomenclature remains resilient. Even the most recent RFPs and specifications use these terms. But times are changing as new generations of designers enter the workforce and design process. For years, the Building Industry Consulting Service International (BICSI) has been defining the MDF as the "Main Cross-Connect" (MCC) and the IDF as the "Telecommunications Room" (TR). For the purposes of this document, the legacy nomenclature will be used in order to avoid confusion.

Every school should have some combination of the following types of facilities dedicated to telecommunications systems:

- Entrance Facilities (Demarc or Cable Vault) – Secured area where incoming service providers terminate their incoming cables for interconnecting with the building infrastructure.
- Main Distribution Facility (MDF) – Large, dedicated room containing head-end and control equipment for all communications systems.
- Intermediate Data Facility (IDF) – Medium sized “closets” or rooms dedicated to communications distribution equipment for distinct sections of the building to satisfy engineering length requirements.

Each school should have a single entrance facility and a primary MDF. Depending upon school size, a facility could have multiple IDFs

- Technology space requirements should be designed and located beginning with the MDF. The MDF should serve as the nerve center of the data, voice and

security systems. The video head-end equipment should be located within or adjacent to the television studio, in schools that have been provided with one. Otherwise, the video head-end should be in or adjacent to the media center.

- For multi-story buildings, an IDF should be present on every floor. Where possible, IDFs should stack on top of one another. IDF location should consider that no individual cable can exceed 300 feet in actual length, including vertical transitions and cable slack.

A. Entrance Facilities

The entrance facility is optimally a dedicated room in which all the outside technology services originate or enter the facility (data, voice, security, CATV or other audio visual).

Entrance facilities should comply with the requirements of TIA/EIA-569A and local utility requirements. These rooms should be designed with all four walls of floor-to-ceiling code compliant plywood and should be provided with base lightning protection. In instances where base building surge suppression and generator power is in the design, it should also be made available for this space.

The entrance facility may be a room separate and apart from the MDF. However, it is preferable to coordinate with the service providers and have service brought directly to the MDF. The design consultant should provide a closed conduit system from the cable entry point directly to the MDF or from the separate entrance facility room. All service providers should clearly identify and label all termination fields per TIA/EIA- 606A.

B. Primary and Secondary Technology Spaces and Equipment Rooms

The following are guidelines for placement, size, environmental requirements, grounding and bonding, cable routing, wall and rack space for the various technology systems.

MAIN DISTRIBUTION FRAME (MDF)

The MDF is a multi-function, secure, climate-controlled space dedicated to the exclusive use of building telecommunications systems. Every school should have a single MDF with the following characteristics or elements:

- Wherever possible it should house entrance facilities and demarcation points for the various telecommunications systems serving the building and the central grounding equipment for the telecommunications equipment.
- Access to this room should be tightly controlled via a non-master key or access control card reader.
- The data, voice, security and intercom/master clock systems should locate their head-end equipment within this facility.
- Consideration should be given to the room's layout to allow for expansion of the data network, location of additional systems as they come online, and possible location of technician work space to repair

equipment, troubleshoot network problems, or assemble new equipment.

- Floor-mounted standard open data equipment racks may be used in spaces where student/staff access is limited, otherwise data equipment cabinets should be used.
- The MDF should be interconnected with all other telecommunications rooms with minimum of two (2) 3-inch conduit assemblies. Guidelines for these conduit systems can be referenced from TIA/EIA-569-A.
- The MDF should be located to minimize the number of IDFs, but not violate the "300-foot rule" (restriction of horizontal cable links to less than 90 meters or approximately 300 feet).

INTERMEDIATE DISTRIBUTION FRAMES (IDF)

IDF design guidelines are as follows:

- Ideally, horizontal Unshielded Twisted Pair (UTP) cables should be designed to run no more than 220 feet horizontally measured from the IDF patch panel to the end-point/termination/jack.
- Consideration should be given for future expansion of telecommunication spaces and other systems without the need to assign new rooms for equipment. Adhering to industry standards for sizing IDFs based upon square footage of service area is recommended.

EQUIPMENT PLACEMENT GUIDELINES

- Allow three (3) feet of clear working space around cross-connect areas and equipment for ease of maintenance.
- Allow at least four (4) feet of clearance from the centerline of equipment racks and cabinets to the walls in front and to the rear of the rack/cabinet.
- Distribution racks and cabinets should be placed with proper consideration to clearances around the equipment, taking into account sources of EMI (electro magnetic interference), technician workspace, and sufficient walkways to avoid accidental disruption of service.
- When IDFs cannot be dedicated to technology equipment, the data equipment should be partitioned away from other material or equipment by use of a lockable separation. If the space cannot be divided, then equipment cabinets for data equipment should be used instead of equipment racks. Equipment that should be located within each IDF/MDF should include:
    - Distribution racks or cabinets for mounting hardware.
    - Termination fields for fiber optic, UTP, and coaxial cables.
    - Switches for the Local Area Network.
    - Amplifiers and other equipment for the CATV Distribution.
    - Rack-mounted Uninterruptible Power Sources (UPS).

OTHER CONSIDERATIONS

The routing of cabling for the telecommunications and security infrastructure requires consideration of shared space with electrical, mechanical and plumbing pathways. Proper environment for active electronics should be maintained and power be available as outlined below.

Pathways:

The pathways for low voltage cable may consist of cable trays, "J-hooks", conduits and chases to provide access to the various classrooms, administrative offices and other areas from the telecommunications equipment rooms. Low voltage cabling requires consideration in the early stages of the project design to ensure proper coordination with other trades.

HVAC:

- MDFs and IDFs should be maintained between 64 °F and 75 °F at all times. The humidity range should be kept between 30% to 55% relative humidity.
- MDFs and IDFs should have an independent air conditioning system separate from the rest of the building HVAC system, especially if the building's system is centralized, and be able to run 24 hours a day, 7 days a week.
- If the rooms are considered unoccupied, outside air (OSA) can be at the minimum, depending on local codes.
- Generally, no heating is required.
- Maintain positive air pressure to avoid ingress of dust and debris.
- The HVAC system should have an emergency power system backup.

Electrical:

- The electrical requirements for equipment such as computers, printers and scanners should be coordinated with the electrical engineer. Voice/data/AV jacks are typically co-located with electrical outlets.
- 30-Amp, twist-lock receptacles are often needed for rack-mounted, UPS equipment. Receptacles should be located within 12" of the rack or cabinet where the UPS should reside.
- When generators are to be installed, load requirements of the voice, data, and security system should be considered. Some schools may wish to have the public address system on emergency power circuits as well.
- The MDF and each IDF should have a minimum of two non-switched, three-wire 120 V AC duplex outlets, each on separate branch circuits (wired for 20 Amp capacity).
- Additional convenience outlets should be located a minimum of 10 inches AFF (above finished floor) at 6-foot intervals around the perimeter of each room.

- For wall-mounted video equipment, provide a duplex receptacle on a dedicated circuit mounted just above the top of the rack, and a duplex receptacle on a dedicated circuit at least 18" AFF in the center of the plywood sheet.
- Emergency lighting and power to MDF/IDF is recommended.
- Telecom power should be on different circuits than lighting fixtures.
- Lighting in MDF/IDF should provide a minimum of 500 lux (50 foot-candles) measured 3 feet AFF. Fixtures should be a minimum of 8.5 feet AFF.
- The school should be provided with a telecommunications grounding and bonding infrastructure designed and installed in accordance with the applicable codes and the latest version of ANSI/TIA/EIA-607, Commercial Building Grounding and Bonding Requirements for Telecommunications. A telecommunications bonding backbone (TBB) should interconnect the telecommunications bonding and grounding infrastructure, through the grounding busbar to the building service ground.

Plumbing/Fire Protection:

- Do not route wet pipes or steam through telecom rooms.
- Dry pipe sprinkler systems are preferred to wet.
- If wet overhead pipes such as drain lines, fire sprinkler lines, and domestic water lines are unavoidable, provide secondary drains below.
- Provide smoke detectors and connect them to the fire alarm system.
- As a first preference, possibly use a chemical fire suppression system such as Ansul 2000 system over a dry pipe sprinkler system.

C. Horizontal Cable

All horizontal cabling must conform to all physical and performance requirements of the current ANSI/TIA/EIA cabling specifications. Category 6 UTP cabling is recommended. Category 5e should be the minimum performance cable installed.

It is beneficial for cable identification and maintenance to use different color cable jackets and jack inserts for different applications. Standards should be established at a district level for uniformity and ease of support. The following color code provides an example for identifying cable and outlet usage:

Gray ……. Voice/Telephone
Blue…….. Data - Computer/Printer/VOIP
Green…… Wireless Access Point (WAP)
Black……..Video (over UTP)
Red ……Security
White ……. Building Control/Management Systems

D. Backbone Cable

All backbone cables should run from the MDF to individual IDFs and terminate in the appropriate cross-connect field. Telephone backbone cabling (for non VoIP phone systems) should terminate in a 110-block mounted on a patch panel within a rack or on fire resistant plywood sheet securely mounted to the wall, both in the MDF and at the destination IDF. Data and voice over IP backbone cabling (typically 6 to 12 strand multimode fiber optic cable) should be terminated in rack-mounted fiber optic patch panels. Single mode fiber may also be used depending on needs and configuration.

While there is no clear standard in copper connectivity, there are industry (TIA) standards for fiber cabling;

Multimode	Orange
Multimode (laser optimized)	Aqua
Single Mode	Yellow
Single Mode (polarized)	Blue

E. Cable Testing, Certification and Warranty

Included within the specifications for cabling systems should be language covering the following:

- Cable length, performance testing, continuity, and standards-based installation.
- Proper pathways installation, with proper support of cables to minimize damage and allow for quick access to the cable pathway.
- Proper labeling at all cross-connects telecom rooms, and service entries.
- Proper environmental conditioning for all telecom rooms: temperature, positive air pressure, humidity levels, lighting, and room layout.
- Proper equipment grounding.
- Equipment to be neatly and properly installed to allow servicing, minimize damage, and maintain clearances as required by code.
- Provision of adequate power has been provided at the proper locations for telecom equipment.
- The entire cable plant from equipment cable at the workstation to the patch cord at the horizontal cross-connect should come with a channel warranty of a minimum 15 years.
- Design consultant should follow the requirements of TIA/EIA-606A to fully provide “as-built” documentation clearly identifying completed IT construction.
- Telecommunications spaces, hardware, and equipment should be permanently labeled. Cables and outlets should also be labeled with a unique identification scheme for each individual cable link. Patch

cords, patch panels and equipment racks should also be uniquely identified.

- Access panels for accessing telecommunications equipment in the ceiling should be uniquely identified on record drawings and labeled accordingly.
- All labeling information should be maintained to reflect as-built and changes documentation. All test documents should reflect the district's standard labeling scheme.

F. Public Address and Clock Systems

The Public Address (PA) clock systems should have the following characteristics and usage.

- The PA system is typically a low voltage system that utilizes a copper cable infrastructure to distribute a user-defined input in a single or bi-directional manner.
- The system should be capable of multiple, simultaneous conversations on separate channels throughout the facility through call-in switches and loudspeaker assemblies.
- A programmable master clock with correction of secondary clocks is typically integrated with the PA system. The master clock system controls tone generation in order to signal class changes.
- The systems are typically microprocessor-based and should be integrated with the telephone system installed within the facility so that with the proper access code, any telephone can access the PA system and make an announcement.
- The system should be expandable to meet the user's future expansion needs and be programmable from a master phone or computer terminal located at the facility.
- The system's main controls should be located in the MDF with only music source and master phones located in the main office location.
- Clock/speaker assemblies are normally located above classroom doorways or at another approved location within the room. Call switches are typically wall-mounted near speaker locations to allow for two-way communications to the main office.
- Ceiling-mounted corridor speakers and wall-mounted clocks should be spaced appropriately to allow easy viewing of clocks and full audio coverage of pages throughout the facility.
- Amplifiers associated with local sound systems in gyms or cafeterias should be equipped and wired so as to mute local speakers when a PA announcement is being made.

G. Physical Security Systems

Security systems can be separated into two major components; access control and surveillance.

Access Control

The following are recommended components and features for access control systems:

- Components should be IP addressable allowing for the use of data cable plant for transport and network accessibility eliminating the need for static "head-end" or monitoring stations. The use of the facility's wireless network can also be considered as devices are available utilizing this technology.
- System should be designed and implemented to control access to the facility, as well as access to certain areas within the facility.
- The access control system should allow restriction levels based on individual needs and shall be an easily programmable, computer-based system.
- The access control system can be used to log and track activity in certain high-value areas of the building, as well as key exterior doors.
- The primary access control components include keypads and card access readers, designed for damage and tamper resistance with a manual key alternative at points of entry.
- Systems utilizing proximity cards rather than card swipe devices are recommended.
- The distribution and control of the keys and access cards should be established and monitored by the security department. In schools without security staff, the main door lock release control should be located in the main office and be accompanied by two-way audio and visual contact, if possible.
- During a fire emergency, the system must unlock all locks and disable any time-delay egress requirements to allow for immediate egress.
- Some schools may consider walk through or hand-held metal detectors.
- All exterior doors should have magnetic locks that are addressable onsite as well as from a remote location in the event that a lockdown or open situation is required.
- Badging systems, with all the necessary equipment required for providing cards, should be included as part of an access control system.
- Secondary means of access control may include exterior gates, exterior barriers, vandal resistant windows and glass, lexan panels and protective metal screens. The inclusion of these additional access control devices must be dependent upon individual facility needs and as deemed necessary by the district.
- Interior protection of the school should include motion detectors, door contacts and glass break sensors.

Video Surveillance

The following are recommended components and features for CCTV systems:

- Components should be IP addressable allowing for use of data cable plant for transport and network accessibility eliminating the need for static "head end" or monitoring stations. The use of the facility's wireless network can also be considered as devices are available utilizing this technology.
- Video surveillance systems should provide visual monitoring of the facility, internally and externally, 24 hours per day. The system should be used to record and provide evidence of incidents and provide a deterrence of further incidents.
- The system should be capable of transmitting over local and wide area networks using TCP/IP protocols.
- Cameras should survey the corridors, specific rooms, main entrance and exit points and all perimeter areas of the facility.
- Digital video recordings should be transmitted from each camera location and stored for a period of time as determined by the district (typically 30 days) on a digital video recorder (DVR).
- IP cameras can utilize unshielded twisted (UTP) cabling (e.g. category 6 cable). Camera locations are wired to an IDF and then utilize the LAN to transmit video over the fiber backbone to the main viewing station at each facility.
- The storage size of the DVRs shall be based upon the number of cameras and selection of recording sequence.
- The recorder should capture digital pictures from each camera at a rate of no less than five frames per second and record data and time for each image.
- Camera images should be accessible through any PC with a network connection and the proper software loaded to view and control the system.
- All cabling associated with the CCTV system should be concealed in conduit in exposed areas or in areas where access is easily available to the general public.
- The location of the main CCTV view station, containing the PC, monitor(s) and camera controls, shall be located based upon type of facility and personnel available to monitor the station. Typically, this location should be either the main security desk or main office.
- Typical camera locations shall be as follows:
    - Exterior cameras should be located at the primary entrance, entrances used by staff and entrances used by the community after school hours.
    - Exterior cameras should be positioned to cover the playgrounds, parking lots, school grounds and roof access locations.

- Interior cameras should be placed outside rooms with sensitive and/or costly equipment susceptible to pilferage or damage such as MDF and IDFs, computer labs, science labs and other labs that have movable, high-value equipment as determined by the district.

H. Audiovisual Systems

Modern audio visual communications need to be integrated and accommodated into the standard telecommunications cable plant. At this point, and for the purposes of this document, most AV systems and components should be described in Division 27, "Communications".

Video Distribution System

The purpose for a video distribution system is to offer video content to learning environments throughout the facility. The system should allow the viewing of various programming from the local cable provider. Internal broadcasting and video distribution could also be possible through video distribution equipment within the school.

The traditional cable medium for video distribution is coax. When engineered properly, this medium provides a robust signal with minimal individual components. An alternate medium is UTP (unshielded twisted pair). With the addition of transmit and receive devices at each end of the twisted pair cable, audio and video signals can be sent over category 5e or 6 cable. If a digital video distribution system is used, video can be transmitted directly over cat 5e or 6 cable.

Presentation/Display Systems

Where called for in the educational specifications and programming documents, instructional spaces should be equipped with some or all of the following components:

- A video projector (mobile or permanently fixed)
- Flat-panel displays (typically in common areas)
- VCR/DVD Player
- Amplifier and speakers
- Projection screen or whiteboard
- Interactive whiteboard

The system should provide the following capabilities.

- Projection of image from a computer to a video projector/projection screen or whiteboard and/or flat-panel monitor.
- Distribution of the audio and video signals from source equipment (e.g. media server, VCR/DVD combo) to the flat panel monitor and/or projector.
- Distribution of the video signals from the school-wide video distribution system to the flat-panel monitor or projector.

Local Sound Systems

Amplified sound systems may be considered for all large, multi-use rooms such as auditoriums, media centers, gymnasiums, cafeterias, multi-purpose rooms (i.e. cafetorium) as well as music rooms. Components may be installed in a wall-mount cabinet or be part of a rolling cart system and may include some or all of the following:

- Speakers
- Microphones (may include hand-held, permanent, wireless)
- Audio Mixer
- Amplifiers
- Source equipment (CD, DVD, PC/laptop etc.)
- Recording capability (where appropriate)

Connection Wall Plates

Wall plates for connection to video distribution, presentation systems and local sound systems should be designed into all instructional areas, shared spaces and specialty rooms. In classrooms they are typically co-located with voice/data and power outlets near the teacher's desk.

Please note that all appropriate space modifications required for the installation and optimization of visual displays and sound systems, including window treatments, lighting controls, power, conduit, cabling and equipment mounting accommodations, should be coordinated with and/or provided in the general construction scope of work and/or the IT or AV systems integrator scope of work.

I. Local Area Network (LAN) Systems

LAN components may include core or chassis type switches, edge or stackable switches, wireless access points (WAPs) and WAP controllers. In addition to data applications, LAN applications can now include audio-video, voice, building management systems (BMS) and security systems.

The proliferation of 802.11 wireless devices and power over Ethernet (PoE) compliant devices has a significant impact on switch requirements. PoE capable switches can support WAPs (wireless access points), voice-over-IP (VoIP) phones, IP based CCTV cameras, IP Speakers (part of the PA system) and other "low-draw" devices via the structured cabling system. As power over Ethernet matures, standards will address the increased power needs of new technology devices.

J. WAN Systems

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations or to the Internet.

Many WANs are built for one particular district and are private. Others are built by Internet service providers or with third party funding/assistance. WANs are

often built using leased lines from either a local phone carrier or cable TV operator.

Some districts have found it economically feasible to build their own private networks by installing fiber optic cables to each school, possibly through a MAN (Metropolitan Area Network). Others are choosing to build a private wireless WAN "mesh network" that connects all the district's facilities without the time or expense of building a physical wired infrastructure.

K. Wireless Systems

Each school should plan their wired infrastructure to include and support wireless access points (WAPs). Care should be taken to implement a security solution to minimize bleed over into the exterior of each building, and to facilitate encryption and control access into the building computer network from roaming users.

It is advisable to include the expertise of an RF (radio frequency) or WiFi consultant in the planning of a wireless system. Given the nature of the materials and design intent, coverage and WiFi design may vary. Generally, one or more wireless site surveys in the project scope (identifying wireless "coverage mapping") will provide adequate planning and coverage when the facility is complete.

In order to ensure that WAPs are able to be located where necessary once the site has been turned over to the school, data jacks should be installed to allow flexibility in the wireless network design. Obstacles that may not be reflected on architectural drawings will interfere with wireless reception. Therefore, at a minimum, all classrooms, office suites, corridors, and common areas should have a minimum of one (1) data drop for a wireless AP. Large open areas such as the cafeteria, gymnasium and media center should have multiple drops for WAPs.

Drops intended for wireless should be located near the ceiling to promote better signal reception once WAPs are activated. Power for the WAPs is typically provided through power over Ethernet equipment.

L. Building Management Systems (BMS)

Building management and control systems include all the systems embedded in buildings that have traditionally used proprietary control standards. Examples of building control systems include: heating, ventilation and air conditioning (HVAC), elevators, laboratory equipment, life/safety systems, access control, intruder detection, A/V devices and event management.

BMS systems are trending away from proprietary networking protocols towards IP. This places an additional "mission critical" application onto the converged data infrastructure. It will become the IT department's responsibility to integrate their systems with the systems that run, manage, and monitor buildings and facilities.

M. Network Security

It is extremely important to carefully plan for the security of the network, its contents and its users. Firewalls are recommended for the local and wide area networks. These "network security" devices should be located in the headend network rack, and be connected to the incoming Internet feed to protect the data network resources. The firewall should provide IP security and virtual private networking capabilities, offer sufficient throughput and the ability to handle multiple concurrent connections and various encryption standards.

The firewall should have a current, upgradeable operating system. All other network security software for PC servers and desktops should be determined by the district. (i.e. anti-virus, network access protection etc.) In addition to this level of security, the district must proactively protect, via Internet filters and other tools, the students from online/Internet threats.

N. Disaster Recovery (DR) and Business Continuation (BC)

Each school, as part of its emergency planning documents, should have a plan for recovering from various levels of disasters and continuing the business of educating its students. Recent school shootings, the terrorist attacks of September 11, 2001, Hurricane Katrina, and pandemic flu threat have emphasized the importance of DR and BC planning.

In a memo to chief school administrators dated September 14, 2006 (see Appendix F for full document), the DOE recommended that districts create a continuity of instruction and core operations plan (CoI/COP). Its purpose is to "insure that a district/school can resume partially or completely interrupted critical functions within a pre-determined time period after a disaster or disruption (e.g. human error, technology failure)."[13]

The referenced memo asks the school district to identify and document essential functions and services and the assets required to deliver those services. This is to be followed by preparing a number of scenarios against which the CoI/COP is to be tested. Lastly, based upon the scenario testing, the plan is to be modified to cover situations discovered during the testing procedure.

O. Convergence

In the past, telecommunications, information technology and broadcasting all operated independently in terms of the technology used, the information transmitted and the networks (cabling) employed. Television, radio, telephones and computers were used for discrete purposes and the services provided were regulated via different systems and standards.

Technological convergence enables traditionally distinct voice, data, security, AV, building control and other transmissions to be transported over the same network and to use integrated cabling infrastructure and devices for purposes such as telephony, television or personal computing. Districts are able to add voice communications, security systems and video distribution to the LAN

[13] From September 14, 2006 memo to Chief school Administrators from Isaac R. Bryant, Deputy Commissioner State of NJ Department of Education. See Appendix F.

configuration and gain the benefits of cabling systems cost savings and reduced infrastructure maintenance costs.

P. IT Commissioning

Commissioning is the process of ensuring that systems, classically heating, cooling, plumbing and electrical, perform as designed and intended. Commissioning is an established, systematic approach that begins with the design phase and lasts through project closeout, building startup and operation by the school district.

With the growing emphasis of technology within construction projects, technology infrastructure is becoming the "4th Utility", along with Mechanical, Electrical and Plumbing, making IT commissioning an important cost-saving engineering discipline in large as well as small projects. Commissioning should be included at the inception of the design process to assure requirements are translated into effective solutions.

Information Technology commissioning should include:

- Wired & Wireless Data Systems
- Telecommunications Voice/Phone Systems
- Audio/Visual Systems
- Security Systems

Each system should have a "Commissioning" paragraph/scope within its respective CSI-section. At the minimum, "testing" and "demonstration" sections should contain criteria that allow the full performance of the system to be visible for compliance review.

This is generally performed by a third party to facilitate quality assurance (QA) and project deliverables.

IT commissioning synchronizes district requirements with design intent and the project implementation process. It also reduces change orders. Other benefits include the adherence to national, state and local standards, and quality control to validate warranties and ensure the long-term performance of the school's infrastructure systems.